AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the subject application:

Listing of Claims:

1. (Currently Amended) A computer system comprising:

~~a central processing unit (CPU);~~

an SRAM (synchronous random access memory) to store trusted software, the trusted software to write an encryption key to protected registers in a chipset; and

the chipset additionally having ~~, coupled to the CPU, including~~ ~~: protected registers; and~~ a host controller to:

transmit the encryption key to a peripheral device;

receive data from the peripheral device; and

~~a bus coupled to the host controller; and~~

if the received data is data encrypted based, at least in part, on the encryption key, the host controller to enable use of a peripheral software stack associated with the peripheral device to process data transmitted from the peripheral device.

~~a peripheral device coupled the bus, wherein trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device upon startup of the computer system to verify that the peripheral device is trustworthy.~~

2. (Canceled)

3. (Canceled)

4. (Currently Amended) The computer system of claim 1 wherein the trusted software writes to the protected registers ~~register~~ to indicate to the host controller the encryption key ~~encrypted data~~ to transmit and response data that is to be received from the peripheral device.

5. – 12. (Canceled)

13. (Currently Amended) A chipset comprising:

~~protected registers; and~~

a host controller to:

transmit an encryption key to a peripheral device;

receive data from the peripheral device ~~coupled to a peripheral device via a bus~~; and

if the received data is data encrypted based, at least in part, on the encryption key, the host controller to enable use of a peripheral software stack associated with the peripheral device to process data transmitted from the peripheral device.

~~wherein trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device to verify that the peripheral device is trustworthy.~~

14. (Canceled)

15. (Currently Amended) The chipset of claim 13 wherein the encryption key ~~encryption data~~ is received from a CPU coupled to the chipset ~~and transmitted to the peripheral device~~.

16. (Currently Amended) The chipset of claim 13 wherein ~~the~~ trusted software writes an encryption key to the protected register to indicate to the host controller the encryption key ~~encrypted data~~ to transmit and response data that is to be received from the peripheral device.

17. (Canceled)

18. (Withdrawn) A method comprising:

generating an encryption key within a computer system using trusted software;

the trusted software writing to trusted registers within the computer system to initiate transmission of the encrypted key to a peripheral device; and

transmitting the encryption key to the peripheral device.

19. (Withdrawn) The method of claim 18 wherein the encryption key is transmitted to the peripheral device while bypassing a memory stack associated with the peripheral device.

20. (Withdrawn) The method of claim 18 further comprising verifying whether the peripheral device is operating based upon the encryption key.

21. - 31. (Canceled)

32. (New) The computer system of claim 1, wherein an operating system determines if the received data is data encrypted based, at least in part, on the encryption key by:

decrypting the data;

comparing the decrypted data to expected response data; and

if the decrypted data matches the expected response data, determining that the received data is encrypted based, at least in part, on the encryption key.

33. (New) The chipset of claim 16, wherein an operating system determines if

the received data is data encrypted based, at least in part, on the encryption key by:

decrypting the data;

comparing the decrypted data to the response data; and

if the decrypted data matches the response data, determining that the received data is encrypted based, at least in part, on the encryption key.

34. (New) The chipset of claim 13 wherein the encryption key is received from the peripheral device.